What Is Claimed Is:

1. A security protocol method comprising:

simultaneously authenticating multiple facets of an endpoint;

combining the multiple facets of the endpoint with a pre-master secret;

cryptographically hashing a platform configuration;

mixing the cryptographically hashed platform configuration with the pre-master secret via hash to generate a master secret; and

encrypting the master secret to authenticate a negotiated channel.

2. The method of claim 1, wherein a platform private key is bound to the platform configuration using a trusted platform device.

3. The method of claim 2, wherein the trusted platform device comprises a processor coupled to a protected storage device.

4. The method of claim 1, wherein cryptographically hashing the platform configuration comprises cryptographically hashing the platform configuration using a secure hashing algorithm.

5. The method of claim 4, wherein the secure hashing algorithm comprises Secure Hashing Algorithm Version 1.0 (SHA-1).

6. The method of claim 1, wherein encrypting the master secret comprises digitally signing the master secret with one or more certified keys.

7. The method of claim 6, wherein one or more certified keys includes a platform key.

8. The method of claim 6, wherein one or more certified keys includes a user key.

9. The method of claim 6, wherein one or more certified keys includes a user key and a platform key.

10. The method of claim 6, wherein the platform configuration includes multiple identities and one or more certified keys includes one or more platform identity keys.

11. The method of claim 6, wherein the platform configuration includes multiple identities and one or more certified keys includes each platform configuration identity key.

12. The method of claim 1, further comprising enabling the encrypted master secret to be decrypted at another endpoint, wherein the master secret is used by each endpoint to generate the session keys.

13. The method of claim 1, further comprising:

exchanging an explanation of the platform configuration hashes following session key negotiations to finalize the authentication;

verifying, at both endpoints, key exchange messages, certificates and platform configuration data; and

authenticating the session if no problems arise during verification.

14. The method of claim 13, further comprising halting the authentication session if problems arise during verification.

15. The method of claim 13, further comprising enabling endpoints to exchange data, wherein each endpoint knows that the platform from the other endpoint has been authenticated using a platform identity that ties to the trusted platform module.

16. A security protocol comprising:

a first handshake phase to issue attestation identity credentials; and

a second handshake phase to authenticate based on the attestation identity credentials issued in the first handshake phase.

17. The security protocol of claim 16, further comprising a session resumption handshake phase to resume a previous session.

18. The security protocol of claim 16, wherein the first handshake phase comprises a registration handshake protocol and the second handshake phase comprises an authentication and attestation protocol.

19. The security protocol of claim 16, wherein the second handshake phase comprises an authentication protocol, wherein the authentication protocol includes platform authentication.

20. The security protocol of claim 16, wherein the second handshake phase comprises an authentication and attestation protocol, wherein the authentication and attestation protocol include platform authentication and platform configuration reporting.

21. The security protocol of claim 16, wherein the second handshake phase comprises an authentication and attestation protocol, wherein the authentication and attestation protocol include user authentication, platform authentication, and platform configuration reporting.

22. The security protocol of claim 16, wherein the attestation identity credential comprises a DAA (Direct Anonymous Attestation) credential.

23. The security protocol of claim 16, wherein the second handshake phase includes multiple identities to utilize during authentication, wherein the multiple identities comprise one or more user identity keys, platform identity keys, platform configuration

register values, and stored measurement logs for a server and client, wherein platform configuration register values are modified to incorporate a handshake state digitally combining a master secret into the platform configuration register values.

24. The security protocol of claim 16, further comprising a session resumption protocol to resume a previous session.

25. A network security handshake exchange method comprising:

receiving a pre-master secret, wherein the pre-master secret contains a nonce generated by a server, the pre-master secret including server platform configuration data in the form of a server stored measurement log;

augmenting the pre-master secret with a hash of server platform configuration register values;

modifying the server platform configuration register values to incorporate a handshake state by measuring the pre-master secret into the server platform configuration register values;

authenticating the modified pre-master secret by digitally signing the modified pre-master secret with a server platform identity key and a server user identity key; and

sending a first message to a client, wherein the message comprises the pre-master secret, the modified pre-master secret, the modified pre-master secret digitally signed with the server platform identity key and the modified pre-master secret digitally signed with the server user identity key.

26. The method of claim 25, wherein the first message further comprises the server platform configuration register values and the server stored measurement log.

27. The method of claim 25, further comprising:

receiving an encrypted master secret from the client via a second message, wherein the encrypted master secret is a modification of the modified pre-master secret;

verifying the second message; and

generating session keys if the second message is verified.

28. The method of claim 27, wherein verifying the second message comprises

determining client platform configuration register values from a client stored measurement log;

determining the modified pre-master secret from information in the second message; and

comparing the determined modified pre-master secret with the modified pre-master secret.

29. A network security handshake exchange method comprising:

receiving a first message from a server, the first message comprising a server modified pre-master secret;

augmenting the server modified pre-master secret with a hash of client platform configuration register values;

modifying the client platform configuration register values to incorporate a handshake state by measuring the server modified pre-master secret into the server platform configuration register values, wherein modifying the client platform configuration results in a master secret;

digitally signing the master secret with a client user key and a client platform key; and

sending a second message to the server, wherein the second message comprises the master secret, master secret digitally signed with the client platform identity key and the master secret digitally signed with the client user identity key.

30. The method of claim 29, wherein the second message further comprises the client platform configuration register values and the client stored measurement log.

31. The method of claim 29, further comprising:

verifying the first message; and

generating session keys if the first message is verified.

32. The method of claim 31, wherein verifying the first message comprises:

determining server platform configuration register values from a server stored measurement log;

determining a pre-master secret from information in the first message; and

comparing the determined pre-master secret with an original pre-master secret, wherein the first message comprises the original pre-master secret.

33. An article comprising: a storage medium having a plurality of machine accessible instructions, wherein when the instructions are executed by a processor, the instructions provide for simultaneously authenticating multiple facets of an endpoint;

combining the multiple facets of the endpoint with a pre-master secret;

cryptographically hashing a platform configuration;

mixing the cryptographically hashed platform configuration with the pre-master secret via hash to generate a master secret; and

encrypting the master secret to authenticate a negotiated channel.

34. The article of claim 33, wherein a platform private key is bound to the platform configuration using a trusted platform device.

35. The article of claim 34, wherein the trusted platform device comprises a processor coupled to a protected storage device.

36. The article of claim 33, wherein instructions for cryptographically hashing the platform configuration comprises instructions for cryptographically hashing the platform configuration using a secure hashing algorithm.

37. The article of claim 36, wherein the secure hashing algorithm comprises Secure Hashing Algorithm Version 1.0 (SHA-1).

38. The article of claim 33, wherein instructions for encrypting the master secret comprises instructions for digitally signing the master secret with one or more certified keys.

39. The article of claim 38, wherein one or more certified keys includes a platform key.

40. The article of claim 38, wherein one or more certified keys includes a user key.

41. The article of claim 38, wherein one or more certified keys includes a user key and a platform key.

42. The article of claim 38, wherein the platform configuration includes multiple identities and one or more certified keys includes one or more platform identity keys.

43. The article of claim 38, wherein the platform configuration includes multiple identities and one or more certified keys includes each platform configuration identity key.

44. The article of claim 33, further comprising instructions for enabling the encrypted master secret to be decrypted at another endpoint, wherein the master secret is used by each endpoint to generate the session keys.

45. The article of claim 33, further comprising instructions for:

exchanging an explanation of the platform configuration hashes following session key negotiations to finalize the authentication;

verifying, at both endpoints, key exchange messages, certificates and platform configuration data; and

authenticating the session if no problems arise during verification.

46. The article of claim 45, further comprising instructions for halting the authentication session if problems arise during verification.

47. The article of claim 45, further comprising instructions for enabling endpoints to exchange data, wherein each endpoint knows that the platform from the other endpoint has been authenticated using a platform identity that ties to the trusted platform module.